IN THE CLAIMS:

1. (currently amended) An authentication apparatus comprising a body, and a partner side paired with the body, the apparatus comprising: a random pulse generator, arranged in the body or the partner side, or in both the body and the partner side, which generates random pulses; a means which outputs authentication data based on both a random pulse voltage and a random pulse interval of the random pulses generated by the random pulse generator; a means which stores authentication data, a communication means which transmits/receives authentication data; and a control means which controls the communication of authentication data and collates authentication data,

wherein ~~the pulse interval of the random pulses is measured using clock pulses and~~ the random pulse generator detects α particles, a beta ray or a gamma ray released by the collapse of an atomic nucleus and generates the random pulses, ~~and~~

wherein the random pulse interval of the random pulses is measured using clock pulses and an interval of the clock pulses is shorter than the interval of the random pulses, and

wherein said authentication data is outputted based on a combination of the random pulse voltage of the random pulses and a number of the clock pulses acquired by measuring the pulse interval of the random pulses.

2. (original) An authentication apparatus according to claim 1, characterized in that the control means receives the authentication data stored in the storage means arranged on the partner side, collates the received authentication data with authentication data of the storage means arranged in the body, and in accordance with the result of collation, authenticates the partner side, and in that upon completion of the authentication, authentication data is updated, and new authentication data thus updated is written in the storage means of the body and the partner side.

3. (original) An authentication apparatus according to claim 1 or 2, further comprising a drive unit control means which controls a drive unit in accordance with the result of collation by the control means.

4. (original) An authentication apparatus according to claim 1 or 2, characterized in that the body is the body of an electronic lock, and the partner side is a key including an IC card.

5. (cancelled)

6. (previously presented) An authentication apparatus according to claim 1, characterized in that an α particle radiator includes ^{241}Am, ^{210}Pb-^{210}Po, ^{210}Po and/or ^{244}Cm, and a beta ray radiator includes ^{210}Pb.

7. (cancelled)

8. (original) An authentication apparatus according to claim 1 or 2, characterized in that the communication means transmits/receives the authentication data by circuit connection due to contact or by infrared light communication or radio communication.

9. (currently amended) An authentication method comprising the steps of: generating random pulses by a random pulse generator arranged in a body or a partner side paired with the body, or in both the body and the partner side; outputting authentication data based on both a random pulse voltage and a random pulse interval of the random pulses generated by the random pulse generator; storing authentication data; transmitting/receiving authentication data;

and controlling the communication of authentication data and collating authentication data,

wherein ~~the pulse interval of the random pulses is measured using clock pulses and~~ the random pulse generator detects α particles, a beta ray or a gamma ray released by the collapse of an atomic nucleus and generates the random pulses, ~~and~~

wherein the random pulse interval of the random pulses is measured using clock pulses and an interval of the clock pulses is shorter than the interval of the random pulses, and

wherein said authentication data is outputted based on a combination of the random pulse voltage of the random pulses and a number of the clock pulses acquired by measuring the pulse interval of the random pulses.

10. (original) An authentication method according to claim 9, characterized in that the control step receives the authentication data stored in a storage means mating unit arranged on the partner side, collates the received authentication data with authentication data of a storage means arranged in the body, authenticates the partner side in accordance with the result of collation, and after completion of authentication, updates authentication data, and writes new authentication data thus updated in the storage means of

the body and the partner side.

11. (original) An authentication method according to claim 9 or 10, further comprising a drive unit control step for controlling a drive unit in accordance with the result of collation in the control step.

12. (cancelled)

13. (previously presented) An authentication method according to claim 9, characterized in that an α particle radiator includes ^{241}Am, ^{210}Pb-^{210}Po, ^{210}Po and/or ^{244}Cm, and a beta ray radiator includes ^{210}Pb.

14. (cancelled)

15. (original) An authentication method according to claim 9 or 10, characterized in that the communication step transmits and receives the authentication data by circuit connection due to contact or by infrared light communication or radio communication.

16. (original) An authentication apparatus according to claim

1 or 2, characterized in that the body or the partner side includes the hardware of a computer, and the partner side or the body including the random pulse generator is mounted integrally with or independently of the hardware of the computer.

17. (original) An authentication method according to claim 9 or 10, characterized in that the body or the partner side includes the hardware of a computer, and the partner side or the body including the random pulse generator is mounted integrally with or independently of the hardware of the computer.

18. (currently amended) A non-transitory computer readable memory medium storing an authentication program, said authentication program comprising: a code to generate random pulses from a random pulse generator arranged in a body or a partner side paired with the body, or in both the body and the partner side partner side; a code to output authentication data based on both a random pulse voltage and a random pulse interval of the random pulses generated by the random pulse generator; a code to store authentication data; a code to transmit/receive authentication data; and a code to control the communication of authentication data and collate authentication data,

wherein ~~the pulse interval of the random pulses is measured using clock pulses and~~ the random pulse generator detects α particles, a beta ray or a gamma ray released by the collapse of an atomic nucleus and generates the random pulses, ~~and~~

wherein the random pulse interval of the random pulses is measured using clock pulses and an interval of the clock pulses is shorter than the interval of the random pulses, and

wherein said authentication data is outputted based on a combination of the random pulse voltage of the random pulses and a number of the clock pulses acquired by measuring the pulse interval of the random pulses.

19. (currently amended) The non-transitory computer readable memory medium storing an authentication program according to claim 18, characterized in that the code to control the communication of authentication data and collate authentication data includes: a code to receive authentication data stored in a storage means arranged on the partner side; a code to collate the received authentication data with authentication data of a storage means arranged in the body; a code to authenticate the partner side in accordance with the result of collation; a code to update authentication data after completion of the authentication; and a

code to write new authentication data thus updated in the storage means of the body and the partner side.